CERN : le premier pirate témoigne

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 25 septembre 2008

Spyworld Actu

Pour le hacker qui avait réussi à briser une première fois les protections de l'organisation, la récente intrusion est le fait d'un groupuscule en mal de notoriété.

A l'ère de la démocratisation d'Internet, les saboteurs de réseaux pullulent. Ils n'épargnent personne, pas même le CERN. Parole de hacker reconverti. Pour avoir été le premier à infiltrer en 2000 le site du Centre, un Romand spécialiste en sécurité et en cryptographie sait de quoi il parle. A l'époque, il ne lui aura fallu que quelques heures pour y parvenir. Non sans avoir préalablement passé plusieurs jours à « casser » des mots de passe.

Talon d'Achille

Mais il y a deux semaines, rebelote. Le jour de la mise en marche du LHC, des pirates informatiques infiltraient à leur tour le CERN. D'origine grecque, les barbouilleurs sont allés jusqu'à « defacer » - l'action de gommer - une page Internet sur le site Web de l'organisation.

Comment s'y sont-ils pris ? Selon le passionné des réseaux, les pirates auraient agi à l'aveuglette. Ils se seraient servis d'un utilitaire dit de « mass-scanning », pour rechercher sur le Web la liste des systèmes vulnérables. Le site du CERN y figurant par hasard, ils en auraient ensuite exploité les faiblesses.

« A l'aide d'un simple cheval de Troie, ils auraient volé le mot de passe d'un scientifique de Fermilab, un centre collaborant avec le CERN, suppose le spécialiste. En se faisant passer pour ce dernier, ils auraient ensuite attaqué le système pour augmenter leurs privilèges afin d'accomplir leur forfait. »

En tant que point de convergence et d'échanges entre scientifiques du monde entier, la sécurité du CERN est liée à celle des autres centres de recherche. « Ils devaient avoir accès aux systèmes depuis des mois et ont profité de la médiatisation liée au LHC pour pousser leur attaque », estime l'expert.

Caractère infantile

S'agissait-il de hackers expérimentés ou d'un groupuscule de novices en mal de notoriété ? Le message de caractère « infantile » laissé sur le site ferait plutôt pencher pour la seconde hypothèse.

« En réalité, ils n'ont fait qu'égratigner la vitrine de l'expérience en elle-même. Pirater le LHC, à proprement parler, c'est une autre paire de manches », conclut l'ancien hacker.

Hackers, crackers où script-kiddies : qui sont ces flibustiers de l'informatique qui écument nos réseaux ? Selon leurs propres définitions, un vrai hacker est d'abord un passionné de l'informatique qui possède des compétences de haut niveau. Il s'introduit de manière ciblée dans les systèmes, non pas pour nuire, mais pour tester ses propres capacités et dénicher d'éventuelles failles de sécurité. Il finit généralement par -prévenir les propriétaires de ses attaques.

Le cracker, lui, a tout du criminel. Il se glisse dans les serveurs pour y détruire des fichiers, voler des données et accéder à des informations financières.

Quant aux script-kiddies, ce sont des filous sans expertise particulière. Ils se désintéressent des architectures compliquées et se servent volontiers de logiciels prêts à utiliser. Ces derniers prolifèrent dans le monde informatique souterrain et sont responsables de la grande majorité des attaques recensées.

Le CERN en a fait les frais, par deux fois en huit ans.

© Keystone | Qui sont ces flibustiers de l'informatique qui écument nos réseaux ?

Post-scriptum :

http://www.tdg.ch/geneve/actu/2008/...